Лабораторная работа № 4

АРХИТЕКТУРА И АДРЕСАЦИЯ СТЕКА TCP/IP

Цель работы

Изучить основные концепции адресации IPv4 и IPv6: структуру IPv4 и IPv6-адреса, понятие и функции маски, диапазоны IP-адресов, принципы создания подсетей, понятие маршрутизации, типы IPv6-адресов, основные технологии перехода на IPv6.

Постановка задачи

1. Изучить основные теоретические вопросы, используя материалы лекций, рекомендуемую литературу и методические указания к лабораторной работе:
   - архитектура стека TCP/IP;
   - структура и диапазоны IPv4-адресов;
   - использование масок, разбиение на подсети;
   - структура IPv6;
   - виды IPv6;
   - технологии перехода на IPv6.
2. Выполнить задания по лабораторной работе согласно вариантам.
3. Ответить на контрольные вопросы.
4. Подготовить отчет по лабораторной работе.

Методические указания

1. Числовые-составные адреса. Структура IPv4-адреса

Во многих случаях для работы в больших сетях в качестве адресов узлов используют числовые составные адреса. Типичным представителями адресов этого типа являются IPv4 и IPv6-адреса.

IPv4 - это 32-битный адрес (4 байта).

Для удобства чтения в технической литературе и прикладных программах IPv4-адреса представляются в виде 4-х десятичных чисел, разделенных точками. Каждое из чисел соответствует одному октету (8 битам) и может иметь значения от 0 до 255. Этот формат называется **точечно-десятичным** (Decimal-Pant Notation).

Например: 10010001.00001010.00100010.00000011
145.10.34.3

В IPv4 адресах используется двухуровневая иерархия. Адрес делится на две логические части. Старшую часть - номер сети и младшую - номер узла. Такое деление позволяет передавать сообщения между сетями только на основании номера сети, а номер узла используется после доставки сообщения в нужную сеть.

Поле номера сети в IP-адресе (ID сети) называется **сетевым префиксом**, оно идентифицирует подсеть.

Номер узла (ID узла) идентифицирует устройство в подсети и назначается независимо от локального адреса узла.

Устройствами, которым назначаются IP-адреса, могут быть сетевые интерфейсы конечных узлов, коммуникационные серверы, порты маршрутизаторов. Конечный узел может входить в несколько IP-сетей, следовательно, может иметь несколько IP-адресов. Т.о., IP-адрес характеризует не отдельный узел, а одно сетевое соединение данного узла.

Чтобы понять, какие из 32 битов являются номером сети, а какие номером узла, используются маски.

2. Маски подсети

Маска – это 32-разрядное двоичное число, которое используется в паре с IP-адресом и содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Т.о. маска используется для определения части IPv4-адреса, которая представляет номер сети.

Маска может быть указана в точечно-десятичной нотации, либо как десятичное число после косой черты вслед за IP-адресом.

Например, маска подсети /16 в представлении с разделительными точками выглядит как 255.255.0.0, а маска подсети /24 - как 255.255.255.0.

Представление с косой чертой, называется представлением бесклассовой междоменной маршрутизации CIDR (Classless Inter Domain Routing).

3. Диапазоны IPv4-адресов

Индивидуальные IPv4-адреса можно разбить на публичный диапазон, частный диапазон, групповые адреса и APIPA. Адреса APIPA используются лишь в качестве временных адресов или для изолированных компьютеров, а публичные и частные диапазоны делятся на блоки, которые можно назначать целым сетям.

3.1 Публичные IPv4-адреса

Каждый IPv4-адрес в Интернете должен быть уникален. Распределение адресного пространства курирует **Группа Администрирования адресного пространства Интернет (Internet Assigned Numbers Authority, IANA).**

IANA делегирует ответственность за распределение адресов региональным регистраторам: Asia-Pacific Network Information Center (APNIC), American Registry for Internet Numbers (ARIN) и Reseaux IP Europeans Network Coordination Centre (RIPENCC).

Затем региональные регистраторы выделяют блоки адресов крупным поставщикам услуг Интернета (Internet Service Provider, ISP), которые предоставляют блоки своего адресного пространства потребителям и небольшим интернет-провайдерам.

3.2 Частные IPv4-адреса

Администрация IANA зарезервировала определенные диапазоны IPv4-адресов в качестве частных адресов. Они никогда не используются в глобальном Интернете. Эти частные IPv4-адреса применяются для узлов сетей, которым нужны коммуникации IPv4 без отображения в Интернет.

Диапазоны частных адресов представлены в таблице.

Начальный адрес	Конечный адрес
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Узлы с частными адресами могут подключаться к Интернету через сервер или маршрутизатор, выполняющий преобразование сетевых адресов NAT. **NAT (Network Address Translation)** - технология **трансляции адресов**– преобразование адресов с помощью специальных таблиц соответствия. В роли маршрутизатора с функцией NAT может выступать компьютер Windows Server 2008 или аппаратный маршрутизатор.

Системы Windows Server 2008 и Windows Vista также включают компонент Общий доступ к Интернету (Internet Connection Sharing, ICS), который обеспечивает упрощенные версии служб NAT для клиентов в частной сети.

Часто публичные адреса назначаются общедоступным серверам, а частные — клиентским компьютерам. Каждая организация, которой требуются коммуникации в Интернете, должна располагать хотя бы одним публичным адресом. Этот адрес может использоваться множеством клиентов посредством NAT и диапазонов частных адресов.

3.3 Автоматические частные IP-адреса (Automatic Private IP Addressing, APIPA)

Если компьютеру автоматически назначается IP-адрес, то по умолчанию в случае недоступности DHCP-сервера всем сетевым подключениям назначаются адреса APIPA. Частные адреса APIPA расположены в диапазоне от 169.254.0.1 до 169.254.255.254. Маска подсети 255.255.0.0.

3.4 ГрупповыеIPv4-адреса

Групповая адресация широко используется в Интернет для доставки информации всем узлам, объединенным в логическую группу. Групповые адреса начинаются с префикса 1110. Значение первого октета у них от 224-х и выше. Они не делятся на номер сети и номер узла - это особый групповой адрес **multicast**. Пакет с адресом multicast должны получить все узлы, которым присвоен данный адрес.

3.5 Специальные IP-адреса

Некоторые IP-адреса зарезервированы для специальных целей. Такие адреса не назначаются конечным узлам и не передаются маршрутизаторами.

1) Адрес 0.0.0.0 обозначает все сетевые интерфейсы данного узла либо шлюз по умолчанию (defaultgateway). В IPv6 это адрес **::**.

2) Если номер сети равен нулю, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел-отправитель.

3) Если все двоичные разряды IP-адреса равны единице(255.255.255.255), то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник пакета. Такая рассылка называется **ограниченным широковещательным сообщением** (limitedbroadcast), т.е. только в пределах той сети, где находится отправитель. Пакет с ограниченным широковещательным адресом никогда не будет пропущен через маршрутизатор. В IPv6 он имеет префикс 1111 1111 и относится к multicast-адресам.

4) Если в поле номер узла назначения все двоичные единицы, то пакет рассылается всем узлам сети с заданным номером сети. Такая рассылка называется **направленным широковещательным сообщением** (broadcast или multicasting). (Например, 192.190.21.255/24)

5) IP-адрес, первый байт которого равен 127, используется для тестирования программ и взаимодействия процессов в пределах локальной машины. Данные при этом не передаются по сети, а опускаются до физического уровня и сразу возвращаются модулям верхнего уровня. Образуется «петля». Поэтому адрес 127.0.0.1 называется **loopback** или **«петля обратной связи».**Достижим только с локальной машины, поэтому называется еще **localhost**. В IPv6 это адрес **::1.**

6) Адрес, у которого в поле номер узла все нули, обозначает пул адресов. (Например, 129.35.0.0/16).

7) Адреса, значение первого байта которых превышает 223 не могут использоваться в качестве номера узла, так как они используются для групповой адресации.

4. Определение маски для подсети заданного размера

При проектировании сети для заданного количества компьютеров может потребоваться определить соответствующую маску подсети.

Вначале нужно определить нужное количество адресов, добавив двойку к количеству компьютеров (один адрес для широковещания, другой будет означать пул адресов). Например, при создании новой локальной сети для отдела из 20 компьютеров, которые будут подключены к корпоративной сети предприятия, необходимо 22 адреса:

20+2=22

Затем нужно определить минимальный адресный блок, соответствующий требованиям сети. Четыре бита позволяют адресовать блок из 16 адресов, пять бит – блок из 32 адресов.

2^4=16, 2^5=32

В нашем примере 22 адреса. Следовательно, для нумерации узлов создаваемой сети нужно отвести адресный блок в 5 двоичных разрядов (это 5 нулей в конце маски).

11111111.11111111.11111111.11100000

8-5=3 (3 двоичные единицы в последнем байте)

24+3=27 или $11100000_2=224_{10}$

Необходимая маска подсети будет /27 или 255.255.255.224.

С помощью этой маски можно выделить подсеть нужного размера (на 20 узлов).

5. Разбиение на подсети

Каждый 32-битовый IPv4-адрес состоит из номера сети и номера узла. Адресный блок, получаемый от интернет-провайдера (или центрального сетевого администратора в разветвленной сети), содержит единый ID сети, который изменить нельзя.

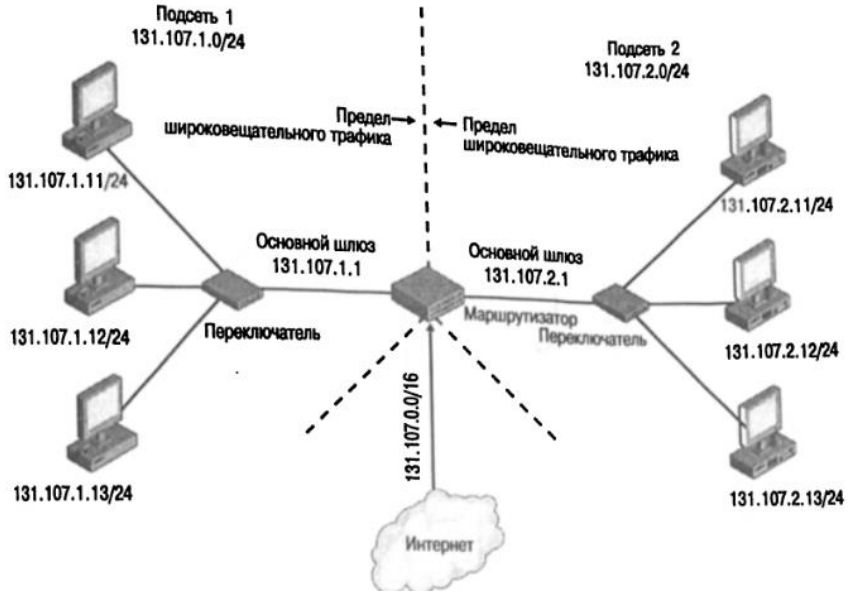
Другими словами, в случае предоставления, к примеру, маски сети 255.255.0.0 значения первых 16 бит адресного блока не конфигурируются. Конфигурируемое адресное пространство представлено лишь в оставшейся части, зарезервированной для ID узла.

Разбиение на подсети — это методика деления адресного сетевого пространства путем добавления битов к маске подсети.

Предположим, вы приобрели у интернет-провайдера для своей организации адресный блок 131.107.0.0/16. Тогда интернет-провайдер использует на своих маршрутизаторах маску подсети /16 (255.255.0.0) для передачи пакетов IPv4 вашей организации по адресам 131.107.y.z.

Пусть внутри организации вы задали маску подсети 255.255.0.0. В таком случае все IPv4-адреса в этом адресном пространствебудут принадлежать одной подсети с номером 131.107.0.0. Мы получим крупную подсеть организации, не разделенную на подсети, включающую 2^{16}-2=65534 узла.

Если заменить используемую маску подсети маской /24 или 255.255.255.0, то новая маска позволит разбить исходное адресное пространство на 256 подсетей по 254 узла в каждой (2^8-2=254).



В то время как исходное адресное пространство /16 состоит из одной подсети, включающей до 65 534 (2^{16} - 2) узлов, новая маска подсети, позволяет разбить исходное пространство на 256 (28) подсетей по 254 (2^8- 2) узла в каждой.

Разбиение на подсети часто применяют, чтобы:

1) обеспечить соответствие физической топологии сети;

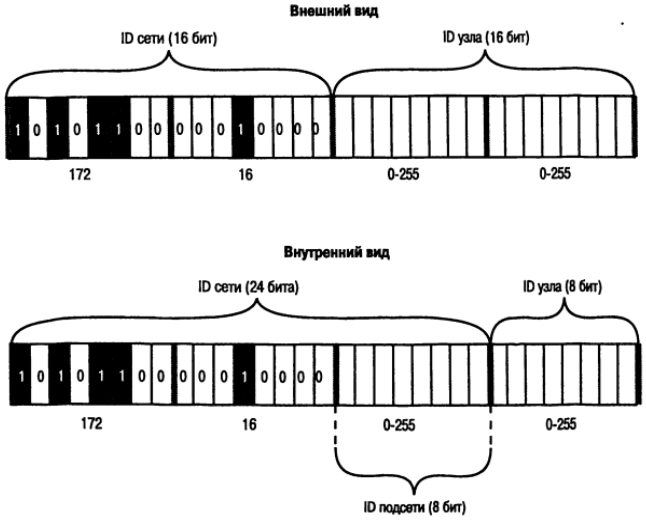
2) ограничить широковещательный трафик в сети;

3) повысить уровень безопасности (путем ограничения неавторизованного трафика за пределами маршрутизаторов);

4) упростить администрирование (благодаря передаче управления подсетями другим отделами или администраторам).

При разбиении сети некоторая часть адресного пространства номера узла добавляется к ID сети. Эти биты используются для внутренней нумерации подсетей в организации (относительно исходного адресного блока) и называются идентификатором подсети.

$$ID_{сети} + ID_{подсети} = \text{расширенный сетевой префикс}$$



Чтобы выяснить, сколько логических подсетей определяется заданной маской подсети используется следующая формула:

$s=2^b$, где s — число подсетей, b — число бит в ID подсети.

6. Адреса IPv6

Версия IPv4 обеспечивает 4,3 млрд возможных уникальных адресов. Для решения проблемы истощения адресного пространства IPv4 была разработана версия IPv6. Вместо 32-битовых адресов версии IPv4 в версии IPv6 используются 128-битовые. Адресное пространство IPv6 обеспечивает 2^{128}, или 340 282 366 920 938 463 463 374 607 431 768 211 456 ($3.4x10^{38}$) уникальных адресов.

По умолчанию протокол IPv6 включен в системы Windows Vista и Windows Server 2008 и виртуально не требует конфигурирования.

IPv6-адреса состоят из восьми блоков по четыре шестнадцатиричных цифры в каждом. Каждый блок отделяется двоеточиями. Пример полного IPv6-адреса:

2001:00B8:3FA9:0000:0000:0000:0003:9C5A

IPv6-адрес можно сократить, исключив все незначащие нули в блоках. Таким образом, предыдущий адрес можно сократить до такого:

2001:DB8:3FA9:0:0:0:D3:9C5A

Затем этот адрес можно еще более сократить, заменив все смежные нулевые блоки двойным двоеточием (::). В отдельном IPv6-адресе это можно сделать только один раз:

2001:DB8:3FA9::D3:9C5A

Поскольку IPv6-адреса состоят из восьми блоков, всегда можно определить, сколько блоков нулей представлены двойными двоеточиями. Например, в предыдущем IPv6-аадресе двойные двоеточия представляют три нулевых блока, поскольку в адресе присутствует пять блоков.

IPv6-адреса разделены на две части: 64-битовый компонент сети и 64-битовый компонент узла. Компонент сети идентифицирует уникальную подсеть, и администрация IANA выделяет эти числа поставщикам ISP или крупным компаниям.

Компонент узла, как правило, основан на уникальном 48-битовом MAC-адресе сетевого адаптера или генерируется случайным образом.

Для одноадресных типов IPv6 не поддерживает идентификаторы подсетей переменной длины, а число битов, используемых для идентификации сети одноадресного типа IPv6-адреса, всегда равно 64 (первая половина адреса). Поэтому для представления одноадресных типов IPv6 нет необходимости указывать маску подсети, поскольку компьютеры распознают идентификатор /64.

IPv6-адреса используют сетевые префиксы, выражаемые в представлении с косой чертой, однако лишь для описания маршрутов и диапазонов адресов, а не для указания ID сети. Например, в таблице маршрутизации IPv6 можно встретить такую запись: 2001:DB8:3FA9::/48.

В отличие от IPv4, версия IPv6 не использует широковещание в сети. Вместо широковещания в IPv6 применяется многоадресная или групповая передача.

Версия IPv6 изначально проектировалась для обеспечения более простого конфигурирования узлов, чем IPv4. Хотя IPv6 можно конфигурировать и вручную (обычно это требуется для маршрутизаторов), конфигурирование IPv6 на компьютерах практически всегда выполняется автоматически. Компьютеры могут получать IPv6-адреса от соседних маршрутизаторов или DHCPv6-серверов. Кроме того, компьютеры всегда сами назначают себе адрес для использования исключительно в локальной подсети.

7. Типы IPv6-адресов

Версия IPv6 описывает три типа адресов: глобальные адреса, канальные и уникальные локальные адреса.

Глобальные IPv6-адреса (GA) аналогичны публичным адресам в сетях IPv4 и используются для области IPv6 Интернета. Для глобальных адресов в настоящее время применяется префикс 2000::/3, который преобразуется в стандартное шестнадцатеричное значение первого блока между 2000 и 3FFF. Например, 2001:db8:21da:7:713e:a426:dl67:37ab.

Канальные адреса (Link-Local Address, LLA) аналогичны автоматически назначаемым частным адресам APIPA (AutomaticPrivateIPAddressing) в IPv4 (например, 169.254.0.0/16). Они конфигурируются самостоятельно и могут использоваться лишь для коммуникаций в локальной подсети. Но, в отличие от адреса APIPA, канальный адрес LLA назначается интерфейсу как вспомогательный даже после получения маршрутизируемого адреса для этого интерфейса. Канальный адрес LLA всегда начинается с fe80. Пример канального адреса- fe80::154d:3cd7:b33b: 1bc 1 % 13

Структура канальногоIPv6-адреса (LLA).

■ Первая половина адреса содержит значение fe80:: (fe80:0000:0000:0000).

■ Вторая половина адреса представляет идентификатор интерфейса.

■ Каждый компьютер помечает канальный адрес идентификатором зоны в формате %ID. Этот ID зоны не является частью адреса и изменяется для каждого компьютера. Идентификатор зоны указывает сетевой интерфейс, подключенный к адресу локально или через сеть.

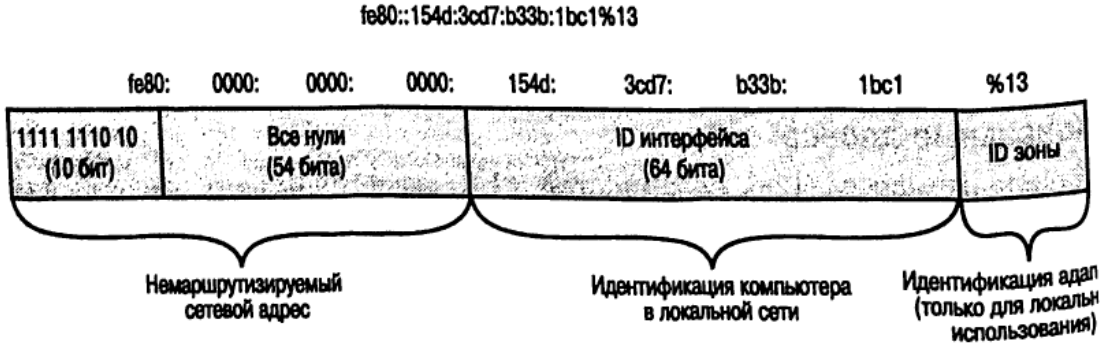


Рисунок – Локальный IPv6-адрес канала

Поскольку все канальные адреса LLA совместно используют один сетевой идентификатор (fe80::), невозможно определить интерфейс, к которому привязан адрес, просто взглянув на него. Поэтому если на компьютере Windows к различным сегментам сети подключено много сетевых адаптеров, эти сети распознаются по числовому значению ID зоны после знака процентов в IP-адресе, как показано в примерах:

- fe80::d84b:8939:7684:a5a4%7
- fe80::462:7ed4:795b:lc9f%8
- fe80::2882:29d5:e7a4:b481%9

Два символа в конце каждого адреса указывают, что сети подключены, соответственно, к зонам 7, 8 и 9. Хотя идентификаторы зон иногда могут использоваться и в других типах адресов, при подключении к локальному IPv6-адресу канала всегда нужно указывать ID зоны. Идентификаторы зон назначаются относительно компьютера, отправляющего сообщение. Чтобы проверить связь с канальным адресом соседнего компьютера с помощью команды ping, нужно указать адрес соседней машины вместе с идентификатором зоны сетевого адаптера на вашем компьютере, который подключен к соседнему компьютеру.

Например, в команде ping fe80::2b0:d0ff:fee9:4143%3 указан адрес интерфейса соседнего компьютера, однако дополнение %3 соответствует идентификатору зоны интерфейса локального компьютера.

В Windows Vista и Windows Server 2008 идентификатор зоны для локального IPv6-адреса канала назначается на основе так называемого индекса сетевого интерфейса. Список индексов интерфейсов на компьютере можно просмотреть, запустив в командной строке команду netsh interface ipv6 show interface.

Уникальные локальные адреса (Unique Local Address, ULA) в IPv6 аналогичны частным адресам в IPv4 (10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16). Эти адреса маршрутизируются между подсетями в частной сети и не маршрутизируются в общественном Интернете. Они позволяют создавать комплексные внутренние сети. Такие адреса начинаются с fd, как, например, локальный уникальный адрес fd65:9abf:efb0:0001::0002.

8. Состояния IPv6-адреса

Узлы IPv6, как правило, автоматически конфигурируют IPv6-адреса, взаимодействуя с IPv6-маршрутизатором. В течение короткого промежутка времени между первым назначением адреса и проверкой его уникальности адрес называется пробным. Компьютеры используют обнаружение дубликатов адресов, чтобы идентифицировать другие компьютеры с тем же IPv6-адресом, отправляя запрос обнаружения соседей (Neighbor Solicitation) с предварительным адресом. Если какой-либо компьютер ответил на запрос, адрес считается недействительным. Если на запрос не ответил ни один компьютер, адрес считается уникальным и действительным. Действительный адрес называется основным в течение срока действия, назначенного маршрутизатором или в автоматической конфигурации. По истечении этого жизненного цикла действительный адрес считается устаревшим. В существующих сеансах коммуникаций может использоваться устаревший адрес.

Задания на лабораторную работу

Упражнение 1.

Какие из данных адресов не могут быть использованы в качестве IP-адреса конечного узла сети, подключенной к Internet? Обоснуйте ответ.

Вариант 1 (7).

1) 0.0.0.0
2) 127.0.0.1
3) 169.254.240.13/16
4) 226.4.37.105
5) 103.24.254.0/8
6) 154.12.255.255/16
7) 255.255.255.255
8) 172.16.12.1
9) 193.256.1.16
10) 194.87.45.0/24

Вариант 2 (8).

1) 228.15.36.103
2) 195.34.116.255/24
3) 161.23.45.305/16
4) 204.0.3.1/24
5) 0.0.0.0
6) 127.0.0.1
7) 169.254.0.10/16
8) 255.255.255.255
9) 123.0.0.0/8
10) 192.168.32.250/24

Вариант 3 (9).

1) 169.254.0.17/16
2) 255.255.255.255
3) 194.12.263.2/24
4) 196.15.241.0/24
5) 116.12.123.5/8
6) 172.16.248.0/16
7) 100.255.255.255/8
8) 127.0.0.2
9) 230.8.38.163
10) 0.0.0.0

Вариант 4 (10).

1) 167.10.255.255/16
2) 129.44.172.3/16
3) 262.194.0.17
4) 127.0.0.3
5) 10.252.14.0/8
6) 225.12.100.4
7) 0.0.0.0
8) 169.254.10.2
9) 255.255.255.255
10) 167.10.0.0/16

Вариант 5 (11).

1) 227.140.10.0
2) 192.168.0.10/24
3) 255.255.255.255
4) 0.0.0.0
5) 132.100.10.110/16
6) 144.12.0.0/16
7) 260.11.0.0
8) 200.192.8.255/24
9) 169.254.101.3/16
10) 127.0.0.5

Вариант 6 (12).

1) 255.255.255.255
2) 0.0.0.0
3) 120.72.0.1/8
4) 125.0.0.0/8
5) 203.10.13.255/24
6) 10.0.0.15/8
7) 229.0.0.14
8) 127.0.0.0
9) 12.302.0.6
10) 169.254.220.30

Упражнение 2. Определение максимального количества узлов подсети

По IP-адресу узла и маске подсети определите номер подсети, номер узла, максимальное число узлов в подсети. Запишите значения в двоичном и десятичном виде.

№ вар	IP-адрес узла и маска подсети	Номер подсети	Номер узла	Максимальное число узлов
1	131.107.17.15/22			
	198.65.12.67, маска 255.255.255.240			
2	10.0.0.5/30			
	129.64.134.5, маска 255.255.128.0			
3	206.73.118.135/26			
	10.10.129.3, маска 255.255.254.0			
4	206.73.118.24/29			
	192.168.23.66 маска 255.255.255.224			
5	10.4.34.3/21			
	131.107.0.10 маска 255.255.255.0			
6	172.16.19.5/22			
	192.168.1.32 маска 255.255.255.128			
7	131.107.100.53/28			
	206.73.118.13 маска 255.255.255.252			
8	10.12.200.169/25			
	192.168.10.9 маска 255.255.248.0			
9	172.20.43.128/24			
	131.107.32.52 маска 255.255.255.240			
10	192.168.244.12/23			
	10.200.53.2 маска 255.255.240.0			

11	131.107.10.13/28			
	172.31.3.24 маска 255.255.255.248			
12	206.73.118.32/27			
	131.107.8.10 маска 255.255.252.0			

Упражнение 3. Определение маски подсети по количеству компьютеров

Каждое значение в левом столбце нижеприведенной таблицы соответствует количеству компьютеров, которое должна поддерживать данная сеть. В правом столбце укажите маску подсети, адресное пространство которой может поддерживать эти компьютеры.

№ вар	Количество сетевых узлов	Маска подсети
1	18	
2	125	
3	400	
4	127	
5	650	
6	7	
7	2000	
8	4	
9	3500	
10	20	
11	32	
12	1500	

Упражнение 4.

По заданному IP-адресу, маске и необходимому количеству подсетей N определить:

- маску для разбиения на подсети;
- список возможных IP-адресов подсетей;
- максимальное количество узлов в каждой подсети;
- минимальный и максимальный IP-адреса для каждой подсети.

№ вар	IP-адрес и маска	Количество подсетей N
1	192.150.148.0/24	6
2	134.234.0.0/16	12
3	134.240.0.0/16	20
4	196.132.14.0/24	3
5	164.20.0.0/16	18
6	220.16.136.0/24	9
7	123.0.0.0/8	100
8	172.16.0.0/16	15
9	120.0.0.0/8	35
10	158.14.50.0/24	7
11	10.0.0.0/8	60
12	126.0.0.0/8	72

Результаты привести в двоичном и десятичном виде и свести в таблицу:

Маска	IP-адреса подсетей	Максимальное количество IP-адресов в подсети	Минимальный IP-адрес в подсети	Максимальный IP-адрес в подсети

Контрольные вопросы

1. Опишите архитектуру стека TCP/IP (количество уровней, соответствие уровней модели OSI, примеры протоколов каждого уровня)?
2. К какому типу адресов относятся IP-адреса?
3. Каков размер IPv4-адреса?
4. Сколько уровней иерархии в IPv4-адресе? Из каких логических частей он состоит? Что такое сетевой префикс?

5. Что такое маска подсети? Как записываются маски и для чего они используются? Что такое VLSM?

6. Как называется адрес 255.255.255.255? Какие узлы получат информацию по такому адресу назначения? Что такое направленное широковещательное сообщение? Почему в сетях TCP/IP широковещательный шторм ограничен?

7. Как можно назначить IP-адрес узлу? Каким еще устройствам назначаются IP-адреса? Может ли конечный узел иметь несколько IP-адресов?

8. Перечислите возможные пути преодоления дефицита IP-адресов.

9. Чем отличаются адреса IPv6? Какова их форма записи?

10. На какие типы делятся IPv6-адреса? Для чего применяется идентификатор зоны в канальных IPv6-адресах? Перечислите возможные состояния IPv6-адреса.